

How do I monitor Agent Health?

Offline/Online Agent Monitoring

Agents Page

On the Agents page, the date and time of the last check-in **per activity** is tracked. Generically speaking, if a software agent is functioning and connected to the Internet, each behavior should have a date of less than a couple hours. Some activities are triggered by activities on the endpoint, while others are set per timers, but with a “jitter” offset of up to 30 seconds, so that customers don’t have surges in network activity.

85753879.png?width=680

Offline Notification Management

To setup notification of offline agents, use the Security Notifications page.

These notifications are intended for the following situations:

1. There is a network issue between an agent, and the Cyber Crucible servers. That can be either due to a firewall (hacker inspired, or just IT operations), or the agent is running but offline. Protection is maintained during offline periods, but security team notifications will not occur until the agent is back online.
2. There is an issue with the Cyber Crucible software. This is very, very rare. Please [open a support ticket](#) with Cyber Crucible immediately, if this occurs.
3. The machine is powered off. This is the most common scenario. Discussion of best practices is next.

85688410.png?width=680

Offline Notification best practices

An important consideration for offline notification, is that a machine which has been powered off, will appear offline to Cyber Crucible’s servers. Workstations, prone to being turned on and off

during normal business operations, would produce offline notifications during lunch breaks, travel between locations, or during holidays.

Best practices for groups already split servers from workstations. Servers are typically best served with shorter offline notification periods, in case of an issue. Workstation focused groups are best for longer periods of appearing offline.

Many Cyber Crucible customers find it best to only create automated notifications for server groups, and periodically filter one of the date fields on the Manage Agents page by a date, such as “Show me agents who have not had their Machine Data Update field updated in the past week”.

85688417.png?width=453

Agents That Are Not Fully Updated

Cyber Crucible agents require a reboot to update. Greater understanding of the update algorithms can be found [here](#). When an agent reports that a reboot will result in an update, the Agents page lists which machines require an update, and are ready to update upon reboot. Sometimes machines, if they are not rebooted often (typically servers), will stage multiple updates before actually upgrading. We see an example of that in the screenshot. The last reboot time is also available.

The weekly Cyber Crucible executive report identifies that number of agents which require an upgrade, and how many of those are ready to upgrade as soon as they are rebooted. The two most common reasons a machine requires an update, but are not ready/staged, are:

1. The machine has been offline, such as an employee on vacation.
2. The machine had a hardware or major software failure/refresh, and Cyber Crucible is actually no longer on that machine.

Other than those two instances, updates normally happen very quickly, and without administrator involvement outside of normal patching and rebooting activities.

85688423.png

Revision #5

Created 2026-05-18 20:26:59 UTC by Dennis Underwood

Updated 2026-07-20 19:21:37 UTC by Dennis Underwood